PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-160876
(43)Date of publication of application : 20.06.1997

(51)Int.CI. G06F 15/00
G06F 13/00
G06F 15/16

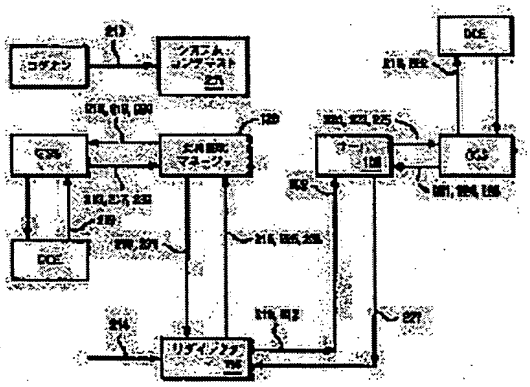
(21)Application number : 08-229538
(22)Date of filing : 30.08.1996

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : KELLS TIMOTHY ROGER
PEEBLES THOMAS FRANK

(30)Priority
Priority number : 95 570463 Priority date : 11.12.1995 Priority country : US

(54) METHOD AND DEVICE FOR MUTUAL CONFIRMATION IN LAN SERVER ENVIRONMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To support decentralized computer mechanisms in LAN server environment by enabling the LAN server machine of a computerized LAN network to pass a generic name security subsystem (GSS) decentralized computer environment (DCE) qualification certificate by making use of an existent mechanism.
SOLUTION: A user logs on first (210) and a log-in context is set as a system context (211). Then an LSCred MGR function acquires the qualification certificate of the user (212) and a GSS qualification certificate is generated from the system context (213). Then a session setup request to the server is generated (214). In a series of steps 215-218, the context token of the server including a GSS call to DCE is acquired. Thus, the LAN server can hand down the qualification certificate by making use to the existent mechanism.



LEGAL STATUS

[Date of request for examination]	28.07.1998
[Date of sending the examiner's decision of rejection]	15.04.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2003-12954
[Date of requesting appeal against examiner's decision of rejection]	09.07.2003
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－160876

(43)公開日　平成９年(1997)６月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ａ
	13/00	３５７			13/00	３５７Ｚ
	15/16	３７０			15/16	３７０Ｎ

審査請求　未請求　請求項の数24　ＯＬ　（全 14 頁）

(21)出願番号　特願平8－229538

(22)出願日　平成８年(1996)８月30日

(31)優先権主張番号　０８／５７０４６３

(32)優先日　1995年12月11日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　ティモシー・ロジャー・ケルス
アメリカ合衆国78681、テキサス州ラウンド・ロック、グレイリング・レーン　3919

(74)代理人　弁理士　合田　潔　（外２名）

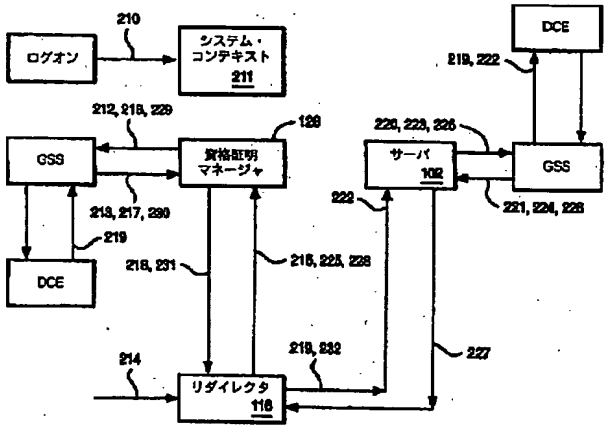
最終頁に続く

(54)【発明の名称】　ＬＡＮサーバ環境における相互確認の方法及び装置

(57)【要約】

【課題】　ＬＡＮサーバ環境において分散コンピュータ機構をサポートする。

【解決手段】　ＬＡＮサーバが、既存の機構を利用して、総称セキュリティ・サブシステム（ＧＳＳ）ＤＣＥ資格証明を渡すことができるように構成される。サーバ管理ブロック（ＳＭＢ）プロトコルが拡張され、サーバはＧＳＳ　ＡＰＩインタフェースを用いて資格証明を獲得及び確認する。ＧＳＳインタフェースが、クライアントとサーバ間で相互確認を達成するために必要な全ての情報をカプセル化するトークンを提供する。こうしたＳＭＢプロトコル拡張に関して、折衝プロトコル（ＮＰ）ＳＭＢにより交換される新たなプロトコル名を含む新たなプロトコル・レベルが定義される。既存のＬＡＮサーバがＮＰ応答内のSMB_secmodeフィールドのビットをオンし、サーバがsecpkgX SMBの交換をサポートすることを示す。サーバは次にSMBsecpkgXまたはSMBsessetupX要求を待機する。



1

【 特許請求の範囲】

【 請求項1 】遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境(ＤＣＥ) 資格証明により、セッション・セットアップの間の相互確認を改良する方法であって、

資格証明を交換するためのサーバ管理ブロック(ＳＭＢ) ・プロトコルの拡張を事前定義するステップと、

前記サーバにより、総称セキュリティ・サブシステム(ＧＳＳ) を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムＡＰＩ インタフェースを通じてアクセスするステップと、

前記アクセスに応答して、前記総称セキュリティ・サブシステムから前記資格証明を獲得し、確認するステップと、

を含む、方法。

【 請求項2 】前記アクセスするステップが、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すステップを含む、請求項1 記載の方法。

【 請求項3 】前記サーバ管理ブロック・プロトコルの拡張が、折衝プロトコル応答内のSMB_secmodeフィールド内の第2 ビットを活動化するステップを含む、請求項2 記載の方法。

【 請求項4 】前記サーバにより、SMBsecpkgX応答を検出するステップと、

前記検出に応答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するステップと、

を含む、請求項3 記載の方法。

【 請求項5 】前記SMBsecpkgX応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義するステップを含む、請求項4 記載の方法。

【 請求項6 】前記クライアントにより、前記サーバに送信する第1 のトークンを獲得するためのGSS_initiate_sec_context機能を呼び出すステップと、

前記クライアントからの前記第1 のトークンに応答して、前記GSS_initiate_sec_context機能に第2 のトークンを転送するステップと、

前記GSS_initiate_sec_context機能により、前記サーバが確認されたか否かを返却するステップと、

を含む、請求項5 記載の方法。

【 請求項7 】前記SMBsecpkgX応答の検出に応答して、前記サーバにより前記第2 のトークンを抽出するステップと、

GSS_accept_sec_context機能により、前記抽出されたトークンを処理するステップと、

2

クライアント確認に応答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信するステップと、

前記SMBsecpkgX応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送するステップと、

前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するステップと、

前記クライアントが前記ネットワークの資源へのアクセスを探索するときのために、前記抽出された資格証明をセッション・データ構造に付加するステップと、

を含む、請求項6 記載の方法。

【 請求項8 】前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記方法が、

資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立するステップを含む、

請求項7 記載の方法。

【 請求項9 】遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境(ＤＣＥ) 資格証明によりセッション・セットアップの間の相互確認を改良する装置であって、

資格証明を交換するためのサーバ管理ブロック(ＳＭＢ) ・プロトコルの拡張を事前定義する手段と、

前記サーバにより、総称セキュリティ・サブシステム(ＧＳＳ) を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムＡＰＩ インタフェースを通じてアクセスする手段と、

前記アクセスに応答して、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認する手段と、

を含む、装置。

【 請求項１０】前記アクセスする手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出す手段を含む、請求項9 記載の装置。

【 請求項１１】前記サーバ管理ブロック・プロトコルの前記拡張のための手段が、折衝プロトコル応答内のSMB_secmodeフィールド内の第2 ビットを活動化する手段を含む、請求項１０記載の装置。

【 請求項1２】前記サーバにより、SMBsecpkgX応答を検出する手段と、

前記検出に応答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換する手段と、

を含む、請求項１１記載の装置。

3

【請求項１３】前記SMBsecpkgX応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義する手段を含む、請求項１２記載の装置。

【請求項１４】前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS_initiate_sec_context機能を呼び出す手段と、

前記クライアントからの前記第1のトークンに応答して、前記GSS_initiate_sec_context機能に第2のトークンを転送する手段と、

前記GSS_initiate_sec_context機能により、前記サーバが確認されたか否かを返却する手段と、

を含む、請求項１３記載の装置。

【請求項１５】前記SMBsecpkgX応答の検出に応答して、前記サーバにより前記第2のトークンを抽出する手段と、

GSS_accept_sec_context機能により、前記抽出されたトークンを処理する手段と、

クライアント確認に応答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信する手段と、

前記SMBsecpkgX応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送する手段と、

前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出する手段と、

前記クライアントが前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加する手段と、

を含む、請求項１４記載の装置。

【請求項１６】前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記装置が、

資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立する手段を含む、

請求項１５記載の装置。

【請求項１７】遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境（ＤＣＥ）資格証明によりセッション・セットアップの間の相互確認を改良するためのコンピュータ・プログラム製品であって、

資格証明を交換するためのサーバ管理ブロック（ＳＭＢ）・プロトコルの拡張を事前定義するコンピュータ読出し可能プログラム・コード手段と、

前記サーバにより、総称セキュリティ・サブシステム（ＧＳＳ）を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムＡＰＩインタフェースを通じてアクセスするコンピュータ読出し可能プログラム・コード手段と、

4

前記アクセスに応答して、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認するコンピュータ読出し可能プログラム・コード手段と、

を含む、コンピュータ・プログラム製品。

【請求項１８】前記アクセスするコンピュータ読出し可能プログラム・コード手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すコンピュータ読出し可能プログラム・コード手段を含む、請求項１７記載のコンピュータ・プログラム製品。

【請求項１９】前記サーバ管理ブロック・プロトコルの拡張のための前記コンピュータ読出し可能プログラム・コード手段が、折衝プロトコル応答内のSMB_secmodeフィールド内の第2ビットを活動化するコンピュータ読出し可能プログラム・コード手段を含む、請求項１８記載のコンピュータ・プログラム製品。

【請求項２０】前記サーバにより、SMBsecpkgX応答を検出するコンピュータ読出し可能プログラム・コード手段と、

前記検出に応答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するコンピュータ読出し可能プログラム・コード手段と、

を含む、請求項１９記載のコンピュータ・プログラム製品。

【請求項２１】前記SMBsecpkgX応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義するコンピュータ読出し可能プログラム・コード手段を含む、請求項２０記載のコンピュータ・プログラム製品。

【請求項２２】前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS_initiate_sec_context機能を呼び出すコンピュータ読出し可能プログラム・コード手段と、

前記クライアントからの前記第1のトークンに応答して、前記GSS_initiate_sec_context機能に第2のトークンを転送するコンピュータ読出し可能プログラム・コード手段と、

前記GSS_initiate_sec_context機能により、前記サーバが確認されたか否かを返却するコンピュータ読出し可能プログラム・コード手段と、

を含む、請求項２１記載のコンピュータ・プログラム製品。

【請求項２３】前記SMBsecpkgX応答の検出に応答して、前記サーバにより前記第2のトークンを抽出するコンピュータ読出し可能プログラム・コード手段と、

GSS_accept_sec_context機能により、前記抽出されたト

5

ークンを処理するコンピュータ読出し可能プログラム・コード手段と、
クライアント確認に応答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信するコンピュータ読出し可能プログラム・コード手段と、
前記SMBsecpkgX応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送するコンピュータ読出し可能プログラム・コード手段と、
前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するコンピュータ読出し可能プログラム・コード手段と、
前記クライアントが前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加するコンピュータ読出し可能プログラム・コード手段と、
を含む、請求項２２記載のコンピュータ・プログラム製品。
【請求項２４】前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記コンピュータ・プログラム製品が、
資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立するコンピュータ読出し可能プログラム・コード手段を含む、
請求項２３記載のコンピュータ・プログラム製品。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はコンピュータ・システムにおける確認（authentication）に関し、特に、クライアント－サーバ・ローカル・エリア・ネットワーク（ＬＡＮ）環境における確認技術に関する。
【０００２】
【従来の技術】通常のＬＡＮにおけるセッションのセットアップでは、プロセスが従来通り発散し、図2に示されるように、クライアント－ユーザ１００及びサーバ１０２がネットワーク・プロトコル１０４（ＮＰ）を折衝する。こうした折衝の間、プロトコル及び関連するプロトコル・レベル２０８が合意され（例えばCORE、ＬＡＮ２．１などに対応）、セッション・キー１０６がクライアント１００に対して決定される。
【０００３】クライアント－ユーザ１００は通常、ユーザＩＤ、名前、及びパスワードなどの情報１１２をサーバ１０２に、より詳細には、リダイレクタ１１６（図５）に伝送する。これはＬＡＮサーバ１０２への（からの）ネットワーク・インタフェースとして機能する。リダイレクタ１１６は本来、ネットワーク・インタフェース、ディスク・ドライブの再転送（redirecting）、及びファイル入出力などの目的を果たす。例えばクライアントがドライブに接続する場合、クライアントにとってそれはローカル・ドライブと思われるかも知れない。しかしながら、リダイレクタは本来、ドライブを管理する実際のファイル・システムにドライブ指定を渡し得るファイル・システムとして機能することにより、要求をクライアントから、ドライブを処理する実際のファイル・サーバに再転送する。こうしたプロセスはクライアントには透過的である。

6

【０００４】従来の動作では、サーバ１０２が通常、次にそのデータベース１１８（図3）を調査し、ユーザＩＤにもとづき、ユーザのパスワード及びセッション・キー１０６（図2）を抽出し、一致が存在したか否かを判断する。存在した場合、サーバ１０２はサーバのローカル・データベース１１８からユーザ定義１２０（図3）をフェッチする。このセッション・キー１０６は本来、タイムスタンプまたは通し番号である。ここでの技法では、本発明の説明の中で明らかとなる理由から、データベース１１８を使用するのではなく、分散コンピュータ環境（ＤＣＥ：Distributed Computing Environment）及び関連するカベロス・レジストリ（Kerberos registry）１２２（図4）を使用し、より詳細には、ユーザ定義が内在するＤＣＥのディレクトリ及びセキュリティ・サーバ（ＤＳＳ）・コンポーネントを使用する。
【０００５】要するに、クライアント１００は分散コンピュータ環境にログオンするとき、プロトコル１０４（図2）を折衝し、その結果、プロトコル・レベル２０８が返却される。ＩＢＭのＬＡＮサーバ・エンタープライズ（ＬＳＥ）製品などの、ＤＣＥを使用する特定のＬＡＮサーバ環境では、ＤＣＥの利用を確認し、従ってＬＡＮに接続するユーザであるためのＤＣＥ資格証明（credentials）を関連付けることが望ましい。なぜなら、これは通常のＬＡＮサーバ確認機構によるよりも、相当に安全な環境であると思われるからである。従って、ログオン時に、サーバ１０２が理解し得るＤＣＥ資格証明を獲得することが望ましく、こうしたＤＣＥ資格証明は通常、遠隔プロシジャ呼び出し（ＲＰＣ）を通じて獲得される。
【０００６】しかしながら、クライアント１００からサーバ１０２にこうしたＤＣＥ資格証明を獲得する機構が提供されないＬＡＮでは、問題が生じ得ることが判明している。より詳細には、例えばＬＳＥ及び類似のＬＡＮ製品では、元来ＲＰＣ呼び出しが利用されないにも関わらず、サーバはセッションのセットアップの間に、ユーザを確認するために、真正の資格証明を獲得する必要がある。こうした資格証明は、ＰＯＳＩＸアクセス制御リスト（ＡＣＬ）により保護されるＬＳＥ資源へのアクセスを決定するために使用される。
【０００７】
【発明が解決しようとする課題】従って、従来のＬＡＮサーバ機構を利用する一方で、現プロトコルによりクラ

7

イアントからサーバに、こうしたＤＣＥ資格証明を獲得する機構を提供する重大な問題が提示される。こうした現プロトコルには、例えばサーバ管理ブロック（ＳＭＢ）・プロトコルなど、通常X/Open協会により定義されるものが含まれる。

【０００８】

【課題を解決するための手段】本発明の好適な実施例では、コンピュータ化ＬＡＮネットワーク内のＬＡＮサーバ・マシンが、それらの既存の機構を利用して、総称セキュリティ・サブシステム（ＧＳＳ：generic security subsystem）分散コンピュータ環境（ＤＣＥ）資格証明を渡すことができるように構成される。X/Openにより定義されるサーバ管理ブロック（ＳＭＢ）・プロトコルが、こうした資格証明の交換を容易にするように拡張される。サーバはＤＣＥにより提供されるＧＳＳ　ＡＰＩインタフェースを用いて、こうした資格証明を獲得及び確認する。ＧＳＳインタフェースは、クライアントとサーバ間で相互確認を達成するために必要な全ての情報をカプセル化するトークンを提供する。

【０００９】好適な実施例では、こうしたＳＭＢプロトコル拡張に関して新たなプロトコル・レベルが定義され、これは特定の実施例では、折衝プロトコル（ＮＰ：negotiate protocol）ＳＭＢにより交換される新たなプロトコル名を含む。ＩＢＭ　ＬＡＮサーバ・エンタープライズ（ＬＳＥ）製品などの既存のＬＡＮサーバは、応答内のSMB_secmodeフィールドのビット（ＬＳＥに関するビット２）をオンし、こうしたビットは、サーバがsecpkgX SMBの交換をサポートすることを示す。サーバは次にSMBsecpkgXまたはSMBsesssetupX要求を待機する。前者の応答は、ユーザ／クライアント及びサーバがＧＳＳトークンを交換し、相互に確認することを可能にし、更に、サーバが複数のパッケージから選択することを可能にする。既存のＬＡＮサーバ製品は、新たなパッケージをSMB_pkgnameの名で定義し、ＬＡＮサーバはこれをＧＳＳ　ＤＣＥトークンを処理するために送信及び認識する。クライアント上のユーザは、SMBsecpkgXが伝送されたとき確認される。なぜなら、確認は、サーバがユーザを追跡するために必要なデータ構造を割り当て、返却するからである。

【００１０】更に本発明によれば、ＧＳＳトークンの処理に関して、クライアント側において、クライアントがサーバに送信するトークンを獲得するためにgss_initiate_sec_context機能が呼び出される。トークンがサーバに送信され、戻りトークンがサーバから受信される。戻りトークンが次にgss_initiate_sec_context機能に渡され、これが次にサーバが確認されたか否かを返却する。サーバが確認されない場合、セッションの確立が終了される。

【００１１】サーバ側では、SMBsecpkgX応答が受信されるとき、トークンがgss_accept_sec_context機能により

8

抽出され、処理される。クライアントが確認されると、クライアントに送信するためのトークンも受信される。トークンはSMBsecpkgX応答により、クライアントに送信される。ＳＭＢを送信後、サーバはユーザの資格証明をＧＳＳトークンから抽出する。資格証明がセッションのデータ構造に付加され、その後、ユーザが資源をアクセスしようとする度に利用される。

【００１２】リダイレクターＧＳＳ間インタフェースに関して、ここで開示される好適な実施例では、ＬＡＮサーバ・リダイレクタは通常、リング０で実行され、ＧＳＳはリング３で実行される。このことは、リダイレクタ及びＧＳＳが直接通信し得ないことを意味する。従って、本発明によれば、資格証明マネージャ・プロセスが媒介として生成される。資格証明マネージャは、起動時にリダイレクタに専用の（captive）スレッドを提供する。ＬＡＮサーバへの接続が形成されるとき、リダイレクタは専用スレッドを用いてＧＳＳトークンを要求し、処理する。資格証明マネージャは、ＬＡＮサーバに現在ログオンされているユーザの資格証明を用いてトークンを獲得する。ユーザ・プロファイル管理（ＵＰＭ）プロセスは、資格証明マネージャにログオン及びログオフ事象を通知する。これは資格証明マネージャが、セッションのセットアップ試行の度に、ＵＰＭに問い合わせること無く、ログオン・ユーザを追跡することを可能にする。

【００１３】

【発明の実施の形態】最初に図１を参照して、本発明が好適に実現され得るネットワーク環境について説明する。図１は、本発明の方法及びシステムを実現するために使用され得るデータ処理システム８を絵的に表している。図示のように、データ処理システム８はＬＡＮ１０及びＬＡＮ３２などの複数のネットワークを含み、各々のＬＡＮは、好適には複数の個々のコンピュータ１２、１２ａ乃至１２ｃ、３０、３１、３３及び３５を含む。（以下、ネットワーク３２内のコンピュータについて述べる場合、コンピュータ３０を任意に参照するが、説明はネットワーク３２内の任意のコンピュータに当てはまる。）コンピュータ１２及び３０は、例えばＩＢＭパーソナル・システム／２（"ＰＳ／２"とも呼ばれる）・コンピュータまたはIBM RISC SYSTEM/6000コンピュータ・ワークステーションなどの、任意の好適なコンピュータを用いて実現される。ここで"RISC SYSTEM/6000"はＩＢＭの商標であり、"パーソナル・システム／２"及び"ＰＳ／２"はＩＢＭの登録商標である。もちろん、当業者には理解されるように、ホスト・プロセッサに接続される複数の高機能ワークステーション（ＩＷＳ）が、こうした各ネットワークにおいて使用され得る。

【００１４】こうしたデータ処理システムにおいて一般的なように、各個々のコンピュータは記憶装置１４及び（または）プリンタ／出力装置１６に接続される。本発

9

明の方法によれば、１つ以上のこうした記憶装置１４が、文書、資源オブジェクト、または実行可能コードなどのオブジェクトを記憶するために使用され、これらのオブジェクトは、データ処理システム8 内の任意のユーザにより周期的にアクセスされ得る。既知のようにして、記憶装置１４内のこうした各オブジェクトは、オブジェクトを例えば個々のコンピュータ１２または３０のユーザに転送することにより、データ処理システム8 を通じて自由に交換され得る。

【００１５】更に図1 を参照すると、データ処理システム8 はメインフレーム・コンピュータ１８などの、複数のメインフレーム・コンピュータを含むことが分かる。これらは、好適には通信リンク２２によりＬＡＮ１０に接続される。メインフレーム・コンピュータ１８は、ＩＢＭから提供されるエンタープライズ・システム・アーキテクチャ／３７０（"ＥＳＡ／３７０"とも呼ばれる）、またはエンタープライズ・システム・アーキテクチャ／３９０（"ＥＳＡ／３９０"とも呼ばれる）コンピュータを用いて実現され得る。アプリケーションに依存して、例えばアプリケーション・システム／４００（"ＡＳ／４００"とも呼ばれる）などの、中型コンピュータも使用され得る。"エンタープライズ・システム・アーキテクチャ／３７０"、"ＥＳＡ／３７０"、"エンタープライズ・システム・アーキテクチャ／３９０"、及び"ＥＳＡ／３９０"は、ＩＢＭの商標であり、"アプリケーション・システム／４００"及び"ＡＳ／４００"は、ＩＢＭの登録商標である。メインフレーム・コンピュータ１８は更に、ＬＡＮ１０の遠隔記憶装置として機能し得る記憶装置２０にも接続され得る。同様に、ＬＡＮ１０は通信リンク２４、更にサブシステム制御ユニット／通信制御装置２６及び通信リンク３４を通じて、ゲートウェイ・サーバ２８に接続され得る。ゲートウェイ・サーバ２８は好適には、ＬＡＮ３２をＬＡＮ１０にリンクする機能を果たす個々のコンピュータまたはI WS である。

【００１６】ＬＡＮ３２及びＬＡＮ１０に関連して上述したように、オブジェクトは記憶装置２０内に記憶され、記憶されたオブジェクトのための資源マネージャまたはファイル・システム・マネージャとしてのメインフレーム・コンピュータ１８により制御され得る。もちろん、当業者には、メインフレーム・コンピュータ１８がＬＡＮ１０から地理的に遠く離れて配置されてもよく、同様にＬＡＮ１０がＬＡＮ３２から遠く離れて配置され得ることが理解されよう。例えば、ＬＡＮ３２がカルフォルニア州に配置され、ＬＡＮ１０がテキサス州に配置され、メインフレーム・コンピュータ１８がニューヨーク州に配置されたりする。

【００１７】本発明の好適な実施例は、データ処理システム8 内に示される様々なコンピュータに組み込まれ得る。

10

【００１８】ＤＣＥの一部であるＤＳＳプロトコルでは、クライアント１００（図2）がレジストリ１２２（図4）にチケットを要求し、これが次にサーバ１０２（図2）に渡される。幾つかのアプリケーションでは、図7 の１２４で示されるようなネット利用（NetUse）をリダイレクタ１１６に発行し、これがプロトコルを開始する。すなわち、本来、ユーザ発行コマンドがクライアント１００をトリガし、サーバ１０２とのセッションをセットアップする。このネット利用に応答して、リダイレクタ１１６は、プロトコル及びセッション・セットアップの折衝のために、X/OpenのＳMB 通信プロトコルに従い、サーバ管理ブロック（ＳMB）を発行する。しかしながら、本発明によれば、ＤＣＥの総称セキュリティ・サブシステム（ＧＳＳ）・コンポーネント１２６（図7）、及び前述の図7 の１１６で示されるリダイレクタを利用するＬＡＮサーバにおいて、要求を資格証明マネージャ１２８を通じてＧＳＳ１２６に伝達する機構を提供する問題が提示される。この機構を実現するために、資格証明マネージャ１２８に対して状態マシン（図8）が定義される。なぜなら、セッションをセットアップするために、資格証明マネージャとリダイレクタとの間でコマンドが交換されるからである。この状態マシンの動作は、図8 に関連して以下で詳述される。

【００１９】X/Openプロトコルにより定義されるＳMB は、本来、ユーザを確認するために使用される機構であるパッケージの概念を提供する自由形式のセキュリティ拡張である。固有のこうしたパッケージが、図7 の１３０などのトークンの受け渡しを提供する本技法において定義されることは、本発明の重要な特徴である。更に図7 を参照すると、このトークン１３０はＧＳＳ１２６から資格証明マネージャ１２８に、そして次にリダイレクタ１１６に渡されるように示される（図6 にも示される）。ここで、リダイレクタ１１６が本来クライアントのコンポーネントであることが思い起こされよう。サーバはこのトークン１３０がＧＳＳパッケージとして受信された後に、これを処理するために、gss_accept_context呼び出し１３３（図6）を発行する。リダイレクタによるトークンの受信は、サーバ１０２に第2 のトークン１３２（図6）を獲得するように指示する。クライアント１００が次にこの第2 のトークン１３２を資格証明マネージャ１２８に、続いてＧＳＳ１２６転送し、この時ＧＳＳがサーバ１０２を確認する。

【００２０】要するに、第1 のトークンがネットワークを通じて転送されるとき、クライアントは本来、それ自身をサーバに証明済みである。証明されていない場合、セッションのセットアップは終了し、一方、証明されている場合には、セッションのセットアップが実行される。サーバは既にクライアントを確認済みであるので、サーバは機能呼び出しをＧＳＳ１２６に発行し、前述のように、定義をユーザのＧＳＳから獲得する。従来のシ

11

ステムでは、前述のように、ユーザを確認するためのユーザ定義１２０を獲得するために、サーバがそれら自身のデータベース（図3の参照番号１１８で示される）を保守した。しかしながら、本発明によれば、ＧＳＳがあらゆるサーバに対して複製されず、また異なるセキュリティ機構がＧＳＳの下で提供され得る。ＤＣＥ拡張によりシステムは資格証明を獲得でき、ユーザが確認されるだけでなく、本システムによればユーザを確認したサーバを知ることができる。ＧＳＳが使用されるが、確認のために実際に下位で使用されるのは、ＤＣＥ内のカベロス機能である。

【００２１】要するに、ここではＤＣＥにより統合される従来のＬＡＮサーバ・ワークステーション及びサーバが、それらの既存の機構を用いて、確認のためにＧＳＳ　ＤＣＥ資格証明を受け渡すことを可能にするシステムが開示される。ここで開示される特定の実施例では、ＩＢＭから提供されるＯＳ／２（商標）オペレーティング・システムを実行するワークステーション及びサーバに対して、変更が成されるが、本発明はこれに限るものではない。代表的なＬＡＮシステムに関する詳細については、"OS/2 Lan Server、Programming Guide and Reference"（著作権I ＢＭ、S10H-9687-00、1994）を参照されたい。しかしながら、上述の概念は、他のオペレーティング・システムを実行するワークステーション及びサーバにも拡張され得る。

【００２２】ＯＳ／２の実施例では、既存のＬＡＮサーバ製品に対する変更が、ＮＰ応答内のsmb_secmodeフィールドの第2ビットをオンする。サーバは次に前述のSMBsecpkgXまたはSMBsesssetupX要求を待機する。前者はもちろん、ユーザ及びサーバがＧＳＳトークンを交換し、相互に確認し合うことを可能にし、これについてはX/Open社から提供される"PROTOCOLS FOR X/OPEN PC INTERWORKING: SMB VERSION 2"、Section 11.2で定義されている。この機能は、サーバが複数のパッケージから選択することを可能にする。

【００２３】SMBsecpkgX要求に続くSMBsesssetupX要求は、長さ０のsmb_apasswdを有し得る。なぜなら確認が既に発生しており、その中のあらゆる内容が無視されるからである。SMBsecpkgX要求が受信されないか、SMBsecpkgX要求内に既知のパッケージが含まれないで受信された場合、smb_apasswdフィールドは、サーバがユーザを確認するための有効パスワードを含まねばならない。この場合、サーバはユーザの資格証明を獲得しなければならない。

12

【００２４】ここで述べられる本発明の実施例によれば、折衝プロトコルが次のように変更されなければならない。secpkgX（上述のsecmodeフィールドのビット番号２）をイネーブルするために、セット・フラグが生成される。更に、サーバがレガシ・クライアント（legacy client）をサポートするか否かを決定する新たなsrvhueristicビットが提供される。レガシ・サポートがオフの場合、サーバは折衝時に、レガシ・プロトコルのセットを提供しない。このことは安全性が不確かなレガシ・クライアントの接続を阻止する。

【００２５】更に前述のように、新たなプロトコル・レベルが定義され、これは特定の技法では、ストリングＬＳＥ１０がワイヤー上を流れることを規定する。クロスーセル・サーバのチケットを獲得するために、ＮＰ応答がサーバのセル名及びその長さを含むように変化する。セル名はドメイン名の後に置かれ、セキュリティ・コンテキストを獲得するときに資格証明マネージャ１２８（図5）により使用される。セル名はクロスーセル確認のために要求されるが、折衝がＬＳＥ１０ストリングに帰着するときのみ送信される。

【００２６】また前述のように、secpkgXの変化が要求される。この機能はX/Open社から提供される前記"PROTOCOLS FOR X/OPEN PC INTERWORKING: SMB VERSION 2"、Section 11.2で定義されている。このフォーマットはここで開示される実施例において使用され、特定の情報が例えばI ＢＭから提供されるＬＳ４．０Ｅなどの、使用される特定のＬＡＮサーバのために定義される。SMB_pkglist構造では、SMB_pkgnameが"ＬＡＮサーバ４．０Ｅ　ＧＳＳ／ＤＣＥトークン"であり、これは前述のように、ＬＳ４．０Ｅサーバ製品が送信または認識する唯一のパッケージである。

【００２７】下記の表では、前述のSMBsecpkgXのデータ構造が、次のように定義される。

【表1】

```
Request Format:
  BYTE   smb__com;          /* 値=7E (????) */
  BYTE   smb__wct;          /* 値=4 */
  BYTE   smb__com2;         /* 2次(X)ｺﾏﾝﾄﾞ、0xFF=none */
  BYTE   smb__reh2;         /* 予約(0でなければならない) */
  WORD   smb__off2;         /* (SMBﾍｯﾀﾞ開始から)次のｺﾏﾝﾄﾞ(@smb_wct) */
                            /* へのｵﾌｾｯﾄ */
  WORD   smb__pkgtype;      /* ﾊﾟｯｹｰｼﾞ・ﾀｲﾌﾟ=0 */
  WORD   smb__numpkge;      /* ﾘｽﾄ内のﾊﾟｯｹｰｼﾞ数 */
  WORD   smb__bcc;
struct   smb__pkglist[*];   /* ﾊﾟｯｹｰｼﾞ・ﾘｽﾄ構造。LS4.0Eの1ﾊﾟｯｹｰｼﾞ・ﾘｽﾄ */
```

13　　14

```
Package List Structure (smb_pkglist) Format:
  WORD   smb__pkgnamlen;   /* パッケージ名の長さ */
  WORD   smb__pkgarglen;   /* パッケージ特有情報の長さ */
  BYTE   smb__pkgname[*];  /* パッケージ名 */
struct   smb__pkgargs[1];  /* LS4.0Eのパッケージ特有情報 */
Package Specific Information (smb_pkgargs) Format:
  DWORD  smb_xp_flags;     /* ビット - セットされると、GSSトークンを伴う応答が */
                           /* 相互確認のために要求される */
  WORD   smb_xp_TokenLen;  /* GSSトークンの長さ */
  BYTE   smb_xp_Token[*];  /* 確認情報を含むGSSトークン */
  BYTE   smb_xp_name[*];   /* 確認されるユーザ名 */
Response Format:
  BYTE   smb_com;          /* 値=7E */
  BYTE   smb__wct;         /* 値=4 */
  BYTE   smb__com2;        /* 2次(X)コマンド、0xFF=none */
  BYTE   smb__reh2;        /* 予約( 0でなければならない) */
  WORD   smb__off2;        /* ( SMBヘッダ開始から) 次のコマンド(@smb_wct) */
                           /* へのオフセット */
  WORD   smb_index;        /* サーバにより選択されるパッケージの番号。 */
                           /* LS4.0Eでは0 */
  WORD   smb_pkgarglen;    /* パッケージ特有情報の長さ */
  WORD   smb_bcc;
struct   smb_pkgargs[1];   /* パッケージ特有情報 */
Package Specific Information (smb_pkgargs) Format:
  DWORD  smb_xp_flags;     /* ビット0、GSSトークンが別の一巡の交換を要求。 */
  BYTE   smb_xp_Token[*];  /* 確認情報を含むGSSトークン */
```

【００２８】図5を参照すると、本システムの基本フローが図式的に示される。最初に、ユーザがログオンし（２１０）、ログイン・コンテキストがシステム・コンテキストとしてセットされる（２１１）。次に、LSCred MGR機能がユーザの資格証明を獲得し（２１２）、ＧＳＳ資格証明がシステム・コンテキストから生成される（２１３）。続いて、サーバへのセッション・セットアップ要求が生成される（２１４）。次の一連のステップ２１５乃至２１８は、ＤＣＥへのＧＳＳ呼び出しを含むサーバのコンテキスト・トークンが獲得されることを表す。

【００２９】次にステップ２１９で、システム・コンテキスト・トークンを含むSMBsecpkg_X呼び出しが送信される。この時点で、サーバは始動時の資格証明を獲得し（２２０、２２１）、SMBsecpkg_Xが受信される（２２２）。次にステップ２２３、２２４で、サーバはGSS_Accept_context機能によりユーザを確認し、ＤＣＥへのＧＳＳ呼び出しを含む応答トークンを受信する。続いてステップ２２５、２２６で、サーバはＧＳＳトークンからＥＰＡＣを抽出する。次に、ＧＳＳコンテキスト・トークンを含むSMBsecpkg_X応答が送信され、受信される（２２７）。次にステップ２２８乃至２３１により示されるように、ＤＣＥへのＧＳＳ呼び出しを含むサーバのコンテキスト・トークンが確認される。最後に、ステップ２３２により示されるように、SMBSessSetup_Xが送信され、受信される。

【００３０】本発明の別の面は、有限のライフタイムを有するトークンを提供する従来の実施例に関連する。トークンが消滅するとき、通常、サーバは自動的にクライアントとの接続を切断する。従って、トークンを周期的にリフレッシュするための特定の手段が必要とされる。

【００３１】本発明によれば、セッションがセットアップされた後、資格証明マネージャ１２８（図5）が、チケットの残りのライフタイムを判断する。消滅の直前に、こうした判断を実施した後、資格証明マネージャ１２８は好適には新たなトークンを獲得し、それをサーバ１０２に転送する。このトークンは図6のトークン２４２として表され、図8の状態マシンにより提供される事象モニタリング機能に関連して、詳細に後述される。

【００３２】現ログオン・ステータスは、資格証明マネージャ１２８がどのようにコンテキストを管理するかに影響する。本来、次に示すように、資格証明マネージャに影響する４つのログオン事象が存在する。

【００３３】第1は、図8に示されるように、ログオン機能２３８である。資格証明マネージャ１２８は、ＤＣＥシステム資格証明を獲得しなければならない。資格証明はログオン実行からインポートされる。次に、ログオフ事象２３６が同様に、資格証明マネージャ１２８に影

15

響する。資格証明マネージャは、ログオン・ユーザのために保持していた全てのセッション情報をクリアしなければならない。ログオフが発生するとき、リダイレクタが全てのセッションをクローズし、使用しているＤＣＥシステム資格証明を解放する。この事象はクリーンアップ及び状態保守のためにも必要とされる。第3に、資格証明リフレッシュ２３４が上述のように提供される。この事象は、資格証明マネージャが資格証明を消滅された状態に遷移することを阻止する。資格証明キャッシュ名は変化しない。システムが既に消滅状態の場合、新たなコンテキスト及びキャッシュ名が獲得される。資格証明マネージャは両方のタイプのリフレッシュを処理する。第4に、図8の参照番号２４０で示されるように、資格証明の消滅が状態マシンに提供される。資格証明が消滅すると、資格証明マネージャ１２８はもはやチケットを獲得できない。資格証明マネージャ１２８は従って、この状態の間に要求が入来すると、エラー・コードをリダイレクタに返却する。ユーザがこの状態になると、資格証明はリフレッシュされ得ずに、新たな資格証明のセットがログオン実行により獲得される。

【００３４】資格証明マネージャ１２８の別の面は、クライアント１００がシャットダウンされるときに言及されるべきである。こうした事象において、リダイレクタ１１６はこれ（例えばネット停止機能）を検出し、その時、リダイレクタ１１６により発行されるクローズ・コマンド（図7の２６０）が、資格証明マネージャ・プロセス１２８を終了させる。システムが再始動されるとき、リダイレクタ１１６はブートに際して明らかに開始される。しかしながら、資格証明マネージャ１２８はＧＳＳの残りが開始されるまで、依然実行されない。ＧＳＳが開始すると、資格証明マネージャ１２８はトークン・コマンド１３０を送信し、これはリダイレクタ１１６内で専用（captive）に保持される。この実行スレッドは次にリダイレクタにより使用され、リダイレクタは接続1コマンド２６２を発行する。接続2コマンド２６４は、スレッドを資格証明マネージャ１２８内において専用に保持する。

【００３５】前述の説明を考慮し、ここで述べられる本発明の技法の追加のファクタは、注目に値する。ＤＣＥ用語では、"資格証明（credentials）"はカベロス・チケット、またはより総称的には、ユーザ及びグループの定義と見なされ得る。ユーザは例えば管理者、ゲスト、ユーザなどのメンバである。こうした資格証明は通常、１プロセス当たりを基本とし（on a per process basis）、各プロセスはいわばそれ自身のプロセスを管理する責任を託される。しかしながら、本発明によれば、資格証明マネージャが、個々のプロセスを管理する全てのネットワーク・システムとして提供される。従って本発明によれば、全てのこうした個々のプロセスは、前記項目の責任が、通常例えば特定のログインの使用のように、プロセス特有であると見なされると想定する限り、ＤＣＥ資格証明がそれらの下で動作していることを考えない。通常、これはアプリケーション毎に固有である。しかしながら本発明によれば、プロセス特有のアプリケーションが様々な呼び出しをするとき、それらがシステム・レベル・ベースで管理され、資格証明マネージャは各々のプロセスが何であるかを知り、トークンを獲得するために適切な資格証明を送信する。

16

【００３６】本発明によれば、セキュリティを管理する比較的異類の機構を実現した2つのソフトウェア・エンティティが、本質的に併合される。より詳細には、本発明はＤＣＥコードと共に既存の機構を利用するＬＡＮサーバ・マシンを提供し、それにより、従来のＬＡＮのこれら2つのエンティティ及びＤＣＥコードが、継ぎ目無く作用するようにまとめられる。セキュリティのＬＡＮ技法が比較的単純な確認を提供し、そして本発明によるＤＣＥ確認を使用する利点の1つが、より複雑な確認機構により、より安全な環境を提供することによることが思い起こされよう。

【００３７】ＬＡＮサーバがＧＳＳ　ＤＣＥ資格証明と共に動作することを可能にする資格証明マネージャ技法の新規の提供に加え、X/Open仕様及びSMBアーキテクチャの一部であるSMBsecpkgXパッケージを使用する本発明のトークンの技法は、新規の結果を提供する。本発明のこの面によれば、定義される新規のパッケージが、相互確認を示すフラグ、前述のトークン、並びにユーザ名を含む。ユーザ名は、通常、ユーザが定義されるセッション・セットアップ時に、後のSMB内で獲得される。SMBsecpkg_Xがセッション・セットアップ時に使用する確認プロトコルの折衝であるのではなく、本発明によれば、確認がセッション・セットアップから上流のSMBsecpkgX機能に移される。

【００３８】その体系的な定義により、セッション・セットアップにおいて、ユーザが確認される。しかしながら、本発明によれば、上述のように確認がSMBより以前に移される。従って、システムがセッション・セットアップに至るとき、セッション・セットアップを達成する作業が実行されるが、確認は要求されない。なぜなら、確認は既に達成されているからである。カスタムSMBsecpkg_Xパッケージの新規の使用を通じて確認が効果的に、あるSMBから別のSMBに移される。しかしながら、このパッケージ機能の従来の利用は、製品がセッション・キーにより暗号化されて送信されるときであり、本発明の特徴は、確認のための異なる機構（例えば異なる暗号化アルゴリズム、キーなど）の指定を所望通りに可能にする。しかしながら本発明の技法は、前述のように、確認をセッション・セットアップから上流のSMBsecpkg_Xパッケージの伝送に移すことを容易にする。

【００３９】本発明は特定の実施例に関連して述べられてきたが、当業者には、本発明の趣旨及び範囲から逸脱

すること無しに、その形態及び詳細における他の変更が可能であることが理解されよう。

【００４０】まとめとして、本発明の構成に関して以下の事項を開示する。

【００４１】（１）遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境（ＤＣＥ）資格証明により、セッション・セットアップの間の相互確認を改良する方法であって、資格証明を交換するためのサーバ管理ブロック（ＳＭＢ）・プロトコルの拡張を事前定義するステップと、前記サーバにより、総称セキュリティ・サブシステム（ＧＳＳ）を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムＡＰＩインタフェースを通じてアクセスするステップと、前記アクセスに応答して、前記総称セキュリティ・サブシステムから前記資格証明を獲得し、確認するステップと、を含む、方法。

（２）前記アクセスするステップが、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すステップを含む、前記（１）記載の方法。

（３）前記サーバ管理ブロック・プロトコルの拡張が、折衝プロトコル応答内のSMB_secmodeフィールド内の第２ビットを活動化するステップを含む、前記（２）記載の方法。

（４）前記サーバにより、SMBsecpkgX応答を検出するステップと、前記検出に応答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するステップと、を含む、前記（３）記載の方法。

（５）前記SMBsecpkgX応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義するステップを含む、前記（４）記載の方法。

（６）前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS_initiate_sec_context機能を呼び出すステップと、前記クライアントからの前記第1のトークンに応答して、前記GSS_initiate_sec_context機能に第2のトークンを転送するステップと、前記GSS_initiate_sec_context機能により、前記サーバが確認されたか否かを返却するステップと、を含む、前記（５）記載の方法。

（７）前記SMBsecpkgX応答の検出に応答して、前記サーバにより前記第2のトークンを抽出するステップと、GSS_accept_sec_context機能により、前記抽出されたトークンを処理するステップと、クライアント確認に応答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信するステップと、前記SMBsecpkgX応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送するステップと、前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するステップと、前記クライアントが前記ネットワークの資源へのアクセスを探索するときのために、前記抽出された資格証明をセッション・データ構造に付加するステップと、を含む、前記（６）記載の方法。

（８）前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記方法が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立するステップを含む、前記（７）記載の方法。

（９）遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境（ＤＣＥ）資格証明によりセッション・セットアップの間の相互確認を改良する装置であって、資格証明を交換するためのサーバ管理ブロック（ＳＭＢ）・プロトコルの拡張を事前定義する手段と、前記サーバにより、総称セキュリティ・サブシステム（ＧＳＳ）を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムＡＰＩインタフェースを通じてアクセスする手段と、前記アクセスに応答して、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認する手段と、を含む、装置。

（１０）前記アクセスする手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出す手段を含む、前記（９）記載の装置。

（１１）前記サーバ管理ブロック・プロトコルの前記拡張のための手段が、折衝プロトコル応答内のSMB_secmodeフィールド内の第2ビットを活動化する手段を含む、前記（１０）記載の装置。

（１２）前記サーバにより、SMBsecpkgX応答を検出する手段と、前記検出に応答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換する手段と、を含む、前記（１１）記載の装置。

（１３）前記SMBsecpkgX応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義する手段を含む、前記（１２）記載の装置。

（１４）前記クライアントにより、前記サーバに送信する第1のトークンを獲得するためのGSS_initiate_sec_context機能を呼び出す手段と、前記クライアントからの前記第1のトークンに応答して、前記GSS_initiate_sec_context機能に第2のトークンを転送する手段と、前記

19

GSS_initiate_sec_context機能により、前記サーバが確認されたか否かを返却する手段と、を含む、前記（１３）記載の装置。

（１５）前記SMBsecpkgX応答の検出に応答して、前記サーバにより前記第2 のトークンを抽出する手段と、GSS_accept_sec_context機能により、前記抽出されたトークンを処理する手段と、クライアント確認に応答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信する手段と、前記SMBsecpkgX応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送する手段と、前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出する手段と、前記クライアントが前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加する手段と、を含む、前記（１４）記載の装置。

（１６）前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記装置が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介として確立する手段を含む、前記（１５）記載の装置。

（１７）遠隔プロシジャ呼び出しを元来サポートしないローカル・エリア・ネットワーク・サーバ環境において相互接続されるクライアントとサーバとの間で、分散コンピュータ環境（ＤＣＥ）資格証明によりセッション・セットアップの間の相互確認を改良するためのコンピュータ・プログラム製品であって、資格証明を交換するためのサーバ管理ブロック（ＳＭＢ）・プロトコルの拡張を事前定義するコンピュータ読出し可能プログラム・コード手段と、前記サーバにより、総称セキュリティ・サブシステム（ＧＳＳ）を前記事前定義済み拡張の機能として、前記分散コンピュータ環境により定義される総称セキュリティ・サブシステムＡＰＩインタフェースを通じてアクセスするコンピュータ読出し可能プログラム・コード手段と、前記アクセスに応答して、前記総称セキュリティ・サブシステムから資格証明を獲得し、確認するコンピュータ読出し可能プログラム・コード手段と、を含む、コンピュータ・プログラム製品。

（１８）前記アクセスするコンピュータ読出し可能プログラム・コード手段が、前記クライアント及び前記サーバにより、前記相互確認を実行するために必要な情報をカプセル化するトークンを取り出すコンピュータ読出し可能プログラム・コード手段を含む、前記（１７）記載のコンピュータ・プログラム製品。

（１９）前記サーバ管理ブロック・プロトコルの拡張のための前記コンピュータ読出し可能プログラム・コード手段が、折衝プロトコル応答内のSMB_secmodeフィールド内の第2 ビットを活動化するコンピュータ読出し可能プログラム・コード手段を含む、前記（１８）記載のコンピュータ・プログラム製品。

20

（２０）前記サーバにより、SMBsecpkgX応答を検出するコンピュータ読出し可能プログラム・コード手段と、前記検出に応答して、前記クライアントと前記サーバとの間で、前記相互確認を達成するための総称セキュリティ・サブシステム・トークンを交換するコンピュータ読出し可能プログラム・コード手段と、を含む、前記（１９）記載のコンピュータ・プログラム製品。

（２１）前記SMBsecpkgX応答に対応する総称セキュリティ・サブシステム／分散コンピュータ環境トークン・パッケージを定義するコンピュータ読出し可能プログラム・コード手段を含む、前記（２０）記載のコンピュータ・プログラム製品。

（２２）前記クライアントにより、前記サーバに送信する第1 のトークンを獲得するためのGSS_initiate_sec_context機能を呼び出すコンピュータ読出し可能プログラム・コード手段と、前記クライアントからの前記第1 のトークンに応答して、前記GSS_initiate_sec_context機能に第2 のトークンを転送するコンピュータ読出し可能プログラム・コード手段と、前記GSS_initiate_sec_context機能により、前記サーバが確認されたか否かを返却するコンピュータ読出し可能プログラム・コード手段と、を含む、前記（２１）記載のコンピュータ・プログラム製品。

（２３）前記SMBsecpkgX応答の検出に応答して、前記サーバにより前記第2 のトークンを抽出するコンピュータ読出し可能プログラム・コード手段と、GSS_accept_sec_context機能により、前記抽出されたトークンを処理するコンピュータ読出し可能プログラム・コード手段と、クライアント確認に応答して、前記サーバにより、前記クライアントに送信する総称セキュリティ・サブシステム・トークンを受信するコンピュータ読出し可能プログラム・コード手段と、前記SMBsecpkgX応答にもとづき、前記総称セキュリティ・サブシステム・トークンを前記クライアントに転送するコンピュータ読出し可能プログラム・コード手段と、前記サーバにより、前記総称セキュリティ・サブシステム・トークンから前記ユーザの資格証明を抽出するコンピュータ読出し可能プログラム・コード手段と、前記クライアントが前記ネットワークの資源へのアクセスを探索するするときのために、前記抽出された資格証明をセッション・データ構造に付加するコンピュータ読出し可能プログラム・コード手段と、を含む、前記（２２）記載のコンピュータ・プログラム製品。

（２４）前記サーバがリダイレクタを含み、前記リダイレクタ及び前記総称セキュリティ・サブシステムが異なるリングで動作し、前記コンピュータ・プログラム製品が、資格証明マネージャ・プロセスを、前記リダイレクタと前記総称セキュリティ・サブシステムとの間の媒介

21

として確立するコンピュータ読出し可能プログラム・コード手段を含む、前記（２３）記載のコンピュータ・プログラム製品。

【図面の簡単な説明】

【図1】本発明が有利に採用され得るコンピュータ・ネットワークの機能ブロック図である。

【図2】プロトコル折衝を図式的に示す図である。

【図3】ユーザ定義を獲得するための、サーバによるデータベースの利用を示す図である。

【図4】ユーザ定義を獲得するための、サーバによるＤＣＥレジストリの利用を示すブロック図である。

【図5】図1のシステムにおいて実現可能な本発明のコンポーネント及び信号フローを示すブロック図である。

【図6】本発明のトークン機構を図式的に示す図である。

22

【図7】本発明の資格証明マネージャ及びリダイレクタを示すブロック図である。

【図8】本発明により採用される状態マシンを示す図である。

【符号の説明】

８　データ処理システム

１２、１２ａ、１２ｂ、１２ｃ、３０、３１、３３、３５　コンピュータ

１４、２０　記憶装置

１６　プリンタ／出力装置

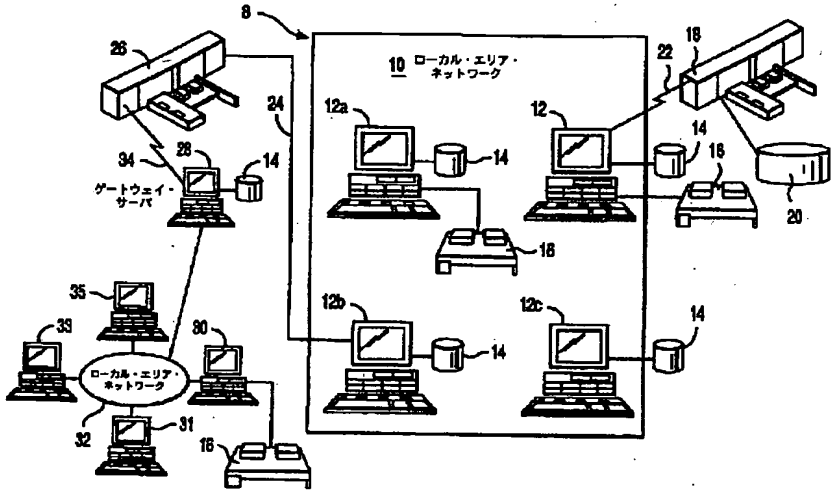
１８　メインフレーム・コンピュータ

２２、２４、３４　通信リンク

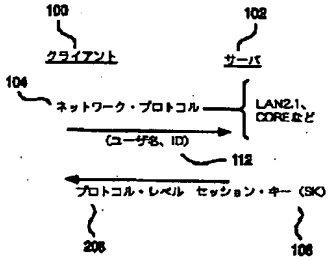
２６　サブシステム制御ユニット／通信制御装置

１１８　データベース

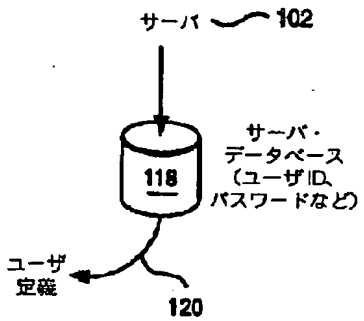
【図1】



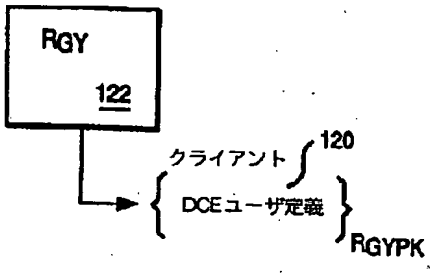
【図2】



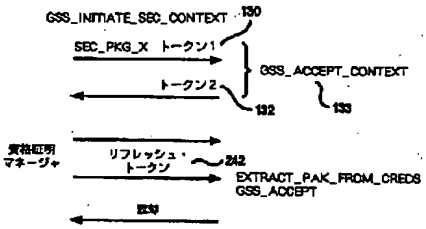
【図3】



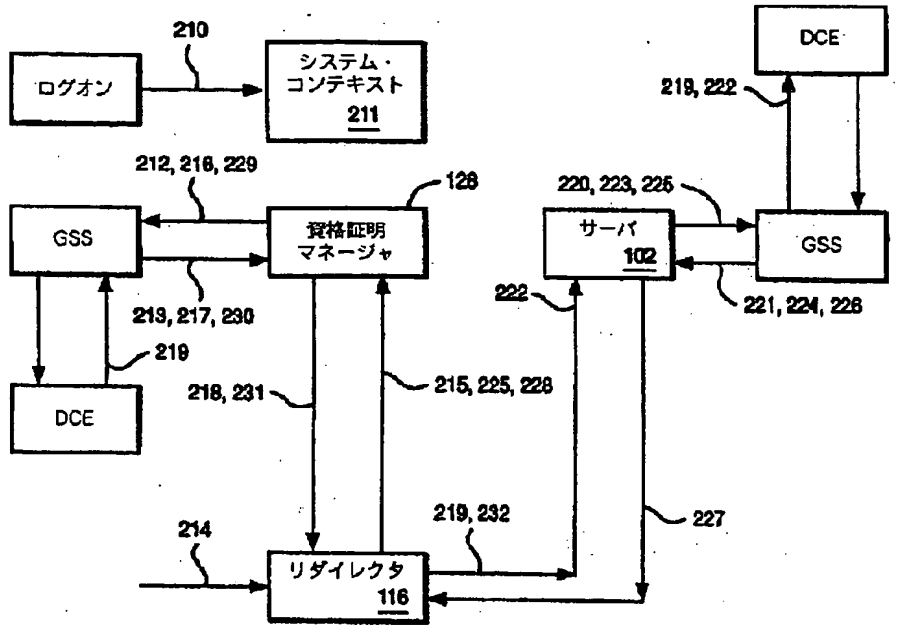
【図4】



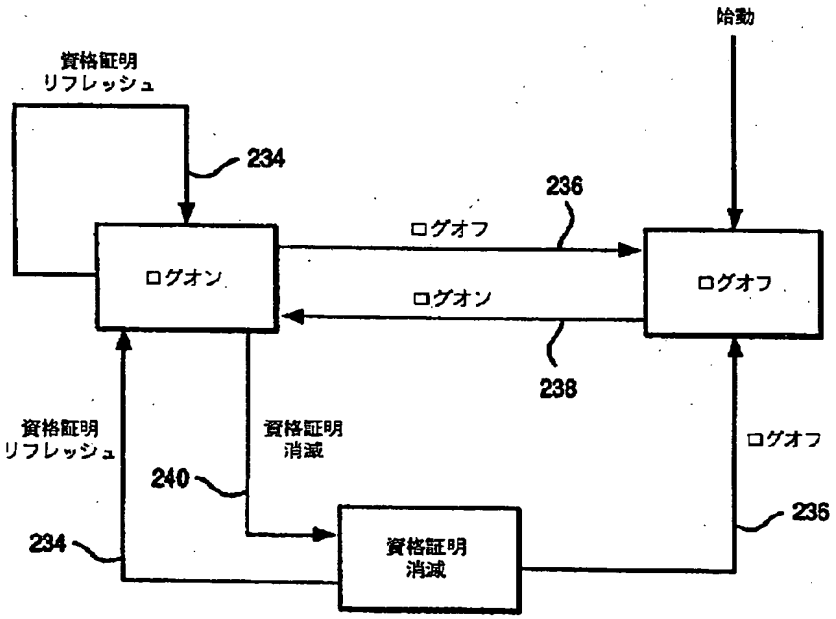
【図6】



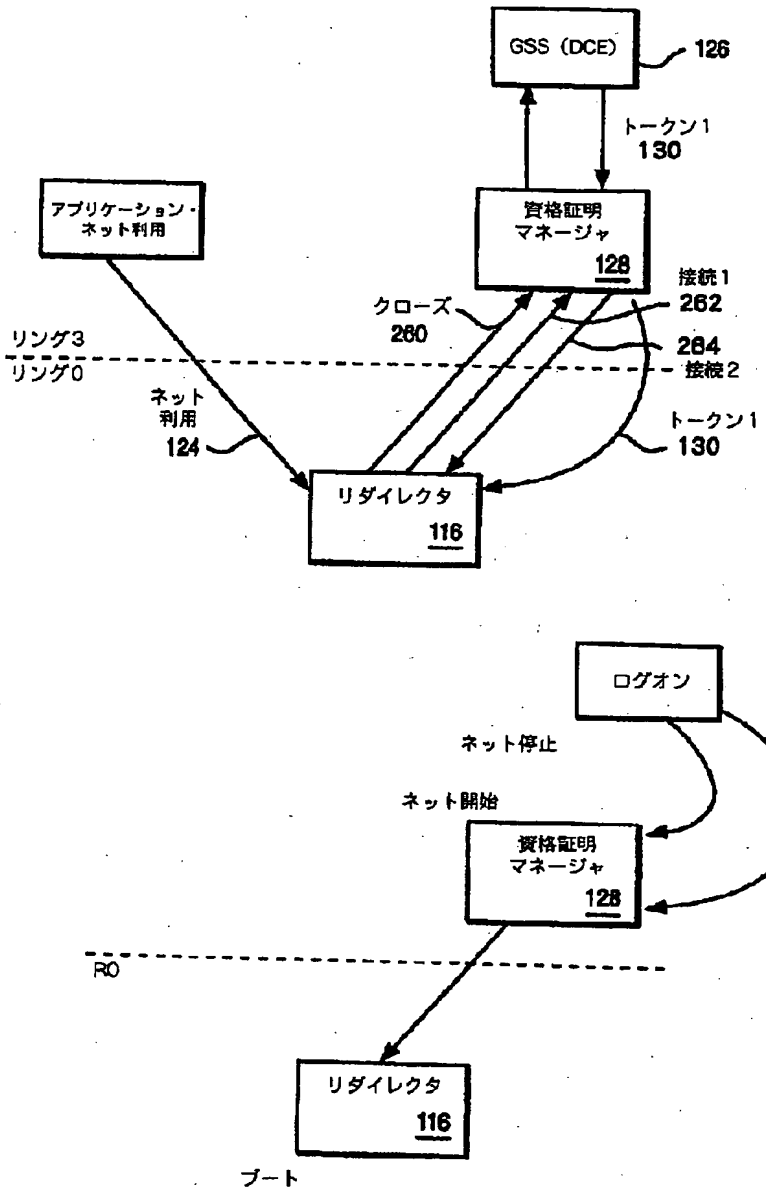
【 図5 】


210
ログオン
システム・
コンテキスト
211
DCE
219, 222
212, 216, 229
128
220, 223, 225
GSS
資格証明
マネージャ
サーバ
102
GSS
222
213, 217, 230
221, 224, 226
219
218, 231
215, 225, 228
DCE
214
219, 232
227
リダイレクタ
116

【 図8 】


始動
資格証明
リフレッシュ
234
236
ログオフ
ログオン
ログオン
ログオフ
238
資格証明
リフレッシュ
資格証明
消滅
ログオフ
240
236
234
資格証明
消滅

【 図7 】



フロント ページの続き

(72)発明者　トーマス・フランク・ピーブルズ
アメリカ合衆国78758、テキサス州オースティン、ソーンワイルド・パス　2323